Information Assurance User Awareness Brief

Contents

- Scope, Definition and Evolution of IA
- Threats
- Malicious Logic
- Classified and Unclassified Information
- User Roles and Responsibilities
- Reporting Procedures

Scope of Information Assurance

- INFOSEC, historically, has included consideration of
  - Hardware and software
  - Operational and accountability procedures
  - Facilities security
  - Physical structures and devices
- The IA concept comprehensively encompasses INFOSEC and other security efforts
- IA includes mechanisms that protect data by ensuring
  - Availability
  - Authentication
  - Confidentiality
  - Non-repudiation
  - Integrity

What Does IA Enable?

- Assures your system will be available when needed
- Assures integrity of data
- Provides confidentiality of data in storage and transit
- Verifies receipt of electronic transactions
- Authenticates participants in electronic commerce

Information Systems Security (INFOSEC)

The protection of Information Systems security against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document,

IA: Relevance to You

- Operational processes at your command
  - Defense Message System (DMS)
  - EKMS
  - SIPRNET
  - CASREPS
  - OPREPS
- Administrative processes at your command
  - Intranet Operations
  - E-Mail Delivery
  - Plan of the Week / Day
  - Record Message Delivery

Evolution of IA

- 1960s
    - Simple security challenges
    - Limited computer usage
- 1970s &1980s
  - Use in homes and battlefields
  - Embedded in weapons systems
- 1990s
  - Computing as utility
  - Dependent on commercial information infrastructure
- 2000 & Beyond
  - Network-centric warfare
  - Enabling technology for electronic commerce
  - Knowledge management
  - Communications, not computing

Threat: Relevance to You

Be aware of the potential threat when you

- Make hardware and software changes
- Use the Internet
- Move information between classified and unclassified systems (Ex.:

- Hackers can enter command information systems to
    - Disrupt information flow
    - Destroy critical software programs
    - Create local account to gain additional information
    - Disable or destroy the information system

Internal Threats

- Unauthorized personnel can gain access to
    - Personnel movements (ex. TAD, PCS)
    - Ship movements (ex. Ports of call, arrival and departure dates)
    - System Administration areas
    - Classified and sensitive information
- Unauthorized personnel hack the system to
    - Gain access to information they are not cleared or have the authority to see
    - Alter their personal records (ex. document completion of a PQS they did not complete)
    - Rewrite their evaluation or fitness report without authorization
    - Alter system parameters for fun

Malicious logic

Hardware, software, or firmware intentionally included in an information system for an unauthorized purpose.

Reference NSTISSI 4009

Types of Malicious logic

- Trojan horse
    - Programs that perform functions not intended by the user
    - Ex.: Program that simulates logon, but actually records user ID and password for later use
- Bombs
    - Trojan horse programs that are triggered by time and date or by a specific condition
    - Ex.: Logic bomb that executes as a particular input sequence is entered or a time bomb that executes on a particular date
- Worms
    - Independent programs that spread copies of themselves to computers

- Backing-up system and application files will help protect you from viruses
- It is a federal offense for a DOD employee to deliberately introduce malicious logic to any information system

Classified Information

Handling Procedures

- Use the same caution for electronic and printed materials
- Store disks and removable media in appropriate storage containers
- Dispose of printed material as prescribed by security regulations
- Secure the terminal and remove all printed information from the work area

Unclassified but Sensitive Information

Handling Procedures

- Ensure authorized personnel have access to the information
- Dispose of waste paper and other materials containing this information into a shredder or burn bag
- Place proper account controls on all system accounts
- Types of Unclassified but Sensitive Information
  - Personnel Records
  - Medical Records
  - Privacy Act Information

User Roles and Responsibilities

General

- Never put classified information on an unclassified system
- Secure the terminal (logging off) before you leave the area
- Lock up media containing sensitive information
- Stay up-to-date with the latest technological changes

User Roles and Responsibilities

Passwords

- Use a mixture of letters and figures in your password
- Do not obvious names for your password
- Memorize your password
- Do not share passwords with co-workers

Reporting Procedures

- Report the problem to your Information System Security Officer (ISSO) for the system you are operating
- Include the following information
    - Location of the terminal you were using
    - Operation you were performing when the problem occurred
    - Nature of the problem
    - Date and Time it occurred
    - Any error messages or report that were displayed
- For perceived incidents, indicate why you believe an incident has occurred

The Bottom Line

- When in doubt, report it!
- Err on the side of caution!